ISSN 0335-3931

norme française

NF ISO/CEI 27001

27 Décembre 2013

Indice de classement : **Z 74-221**

ICS : 35.040

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

E : Information technology — Security techniques — Information security management systems — Requirements
D : Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen

Norme française homologuée

par décision du Directeur Général d'AFNOR.

Remplace la norme homologuée NF ISO/CEI 27001, de décembre 2007.

Correspondance

Le présent document reproduit intégralement la Norme internationale ISO/CEI 27001:2013.

Résumé

Le présent document spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. Il comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation.

Descripteurs

Thésaurus International Technique : traitement de l'information, protection de l'information, sécurité, information, évaluation, danger, défaillance, fraude, accès usager réseau, authentification, cryptographie, gestion, mise en oeuvre, maintenance, contrôle, exigence.

Modifications

Par rapport au document remplacé, révision technique de la norme.

Corrections

Éditée et diffusée par l'Association Française de Normalisation (AFNOR) — 11, rue Francis de Pressensé — 93571 La Plaine Saint-Denis Cedex
Tél. : + 33 (0)1 41 62 80 00 — Fax : + 33 (0)1 49 17 90 00 — www.afnor.org

La norme

La norme est destinée à servir de base dans les relations entre partenaires économiques, scientifiques, techniques et sociaux.

La norme par nature est d'application volontaire. Référencée dans un contrat, elle s'impose aux parties. Une réglementation peut rendre d'application obligatoire tout ou partie d'une norme.

La norme est un document élaboré par consensus au sein d'un organisme de normalisation par sollicitation des représentants de toutes les parties intéressées. Son adoption est précédée d'une enquête publique.

La norme fait l'objet d'un examen régulier pour évaluer sa pertinence dans le temps.

Toute norme est réputée en vigueur à partir de la date présente sur la première page.

Pour comprendre les normes

L'attention du lecteur est attirée sur les points suivants :

Seules les formes verbales **doit et doivent** sont utilisées pour exprimer une ou des exigences qui doivent être respectées pour se conformer au présent document. Ces exigences peuvent se trouver dans le corps de la norme ou en annexe qualifiée de «normative». Pour les méthodes d'essai, l'utilisation de l'infinitif correspond à une exigence.

Les expressions telles que, **il convient et il est recommandé** sont utilisées pour exprimer une possibilité préférée mais non exigée pour se conformer au présent document. Les formes verbales **peut et peuvent** sont utilisées pour exprimer une suggestion ou un conseil utiles mais non obligatoires, ou une autorisation.

En outre, le présent document peut fournir des renseignements supplémentaires destinés à faciliter la compréhension ou l'utilisation de certains éléments ou à en clarifier l'application, sans énoncer d'exigence à respecter. Ces éléments sont présentés sous forme de **notes ou d'annexes informatives**.

Commission de normalisation

Une commission de normalisation réunit, dans un domaine d'activité donné, les expertises nécessaires à l'élaboration des normes françaises et des positions françaises sur les projets de norme européenne ou internationale. Elle peut également préparer des normes expérimentales et des fascicules de documentation.

Si vous souhaitez commenter ce texte, faire des propositions d'évolution ou participer à sa révision, adressez vous à <norminfo@afnor.org>.

La composition de la commission de normalisation qui a élaboré le présent document est donnée ci-après. Lorsqu'un expert représente un organisme différent de son organisme d'appartenance, cette information apparaît sous la forme : organisme d'appartenance (organisme représenté).

Sécurité des systèmes d'information AFNOR CN 27 SSI

Composition de la commission de normalisation

Président : M QUEMARD

Secrétariat : M SOLBES — AFNOR

M	AYADI	DELOITTE CONSEIL
M	BARBUT	CREDIT AGRICOLE SA - AGENCE EVERGREEN (CFONB)
M	BARRAL	BACTECH
M	BENSALEM	BENSALEM NORBERT
M	BERAUD	MICROSOFT FRANCE
M	BILLOIS	SOLUCOM
M	BLAD	OPPIDA
M	BORGHESI	CECURITY.COM
M	BOUCHET	LSTI
M	BOURNON	MORPHO
M	CAIRE	RATP
M	CAZUC	HAPSIS
M	CHAUDRON	SGDSN
MME	COAT	SGDSN
M	COLAS	MICROSOFT FRANCE
MME	COSSARD	CLUB 27001
M	COUTANT	AMOSSYS
MME	DE VISME	INSERM - CIC NANTES MAISON RECHERCHE EN SANTE
M	DELVAUX	MORPHO
M	DUBOIS	THALES COMMUNICATIONS & SECURITY SAS
M	DUBUISSON	ORANGE
MME	FOURATI	EDF R&D
M	GASCON	GIE SESAM VITALE
M	GASTON	GEMALTO SA
M	GAUTIER	GROUPEMENT DES CARTES BANCAIRES
MME	GODIN	ENIGMA SERVICES
MME	GOUGET	GEMALTO SA
M	GOURJAULT	MORPHO
M	GRALL	CNIL
M	GUERIN	GEMALTO SA
M	GUILLOTEAU	ORANGE
M	HOUZÉ	MICROSOFT FRANCE
M	IACOLARE	SYNERTAL
MME	JAMBERT	CNIL
M	JARDIN	CGI BUSINESS CONSULTING FRANCE
M	JOUAS	CLUSIF
MME	JUANALS	BIBLIO UNIV PARIS OUEST NANTERRE DEFENSE
M	LAROCHE	DGSIC
MME	LE	MORPHO
MME	LE GOFF	SOLUCOM

M	LE GRAND	CNIL
M	LOREK	LOREK CONSULTING
M	LUCOTTE	SGDSN
M	MARECHAL	HAPSIS
M	MENNELLA	ALSTOM GRID
M	MICHEL	AMOSSYS
M	MISARSKY	ORANGE
M	MOURER	ATEXIO
M	OURAGA	HAPSIS
M	PAILLIER	CRYPTOEXPERTS
M	PALADINI	AFNOR TEST
M	PEGLI	SRC SOLUTION
MME	PEIRANI	GEMALTO SA
M	PELIKS	CASSIDIAN SAS - EADS FRANCE
M	PINKAS	DP SECURITY CONSULTING
M	QUEMARD	CASSIDIAN SAS - EADS FRANCE
M	RICHY	ORANGE
M	ROCHE	SGDSN
M	SAULIERE	MICROSOFT FRANCE
M	SCHAUER	CLUB 27001
M	SCHAUER	HERVE SCHAUER CONSULTANTS
M	SIMASOTCHI	TEAMUP CONSULTING
M	SITBON	EDF R&D
M	STAIQULY	GIE SESAM VITALE
M	TARRAGO	EDF R&D
M	TRAORE	ORANGE
MME	TRAVERS-VIAUD	BULL SAS (CLUSIF)
MME	TROTIN	LSTI
M	VERGEZ	DELOITTE CONSEIL
M	VERNEUIL	INSIDE SECURE SA
M	VODZISLAWSKY	OPPIDA SUD
M	VOISIN	MICROSOFT FRANCE
M	YSNEL	LOGICA BUSINESS CONSULTING FRANCE

Avant-propos national

Afin de restituer au mieux les différentes acceptions utilisées sur le terrain, l'emploi d'une double traduction a été privilégié pour les termes suivants qui peuvent être rendus respectivement par :

— Asset : actif / bien ; maintien dans le texte de « actif » ;

— Business : affaire / métier ; maintien dans le texte de « métier » ;

— Management : gestion / management ; maintien dans le texte de « gestion », sauf dans le cas de « système de management de la sécurité de l'information » ;

— Organization : organisme / organisation ; maintien dans le texte de « organisation » ;

— Risk management : gestion des risques / management des risques ; maintien dans le texte de « gestion des risques ».

NOTE La traduction des termes relatifs aux risques peut être faite indifféremment au singulier ou au pluriel car « risk » est un terme englobant. Toutefois, préférence est donnée au maintien dans le texte du pluriel « risques ».

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27001 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27001:2005), qui a fait l'objet d'une révision technique.

0 Introduction

0.1 Généralités

La présente Norme internationale a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

La présente Norme internationale peut être utilisée par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans la présente Norme internationale ne reflète pas leur importance, ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/CEI 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/CEI 27003,[2] l'ISO/CEI 27004[3] et l'ISO/CEI 27005[4]) avec les termes et les définitions qui s'y rapportent.

0.2 Compatibilité avec d'autres systèmes de management

La présente Norme internationale applique la structure de haut niveau, les titres de paragraphe identiques, le texte, les termes communs et les définitions fondamentales définies dans l'Annexe SL des Directives ISO/CEI, Partie 1, Supplément ISO consolidé, et, par conséquent, est compatible avec les autres normes de systèmes de management qui se conforment à l'Annexe SL.

Cette approche commune définie dans l'Annexe SL sera utile aux organisations qui choisissent de mettre en œuvre un système de management unique pour répondre aux exigences de deux ou plusieurs normes de systèmes de management.

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

1 Domaine d'application

La présente Norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. La présente Norme internationale comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente Norme internationale.

2 Références normatives

Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions fournis dans la norme ISO/CEI 27000 s'appliquent.

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui influent sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.

NOTE Déterminer ces enjeux revient à établir le contexte externe et interne de l'organisation étudié dans le paragraphe 5.3 de l'ISO 31000:2009.[5]

4.2 Compréhension des besoins et des attentes des parties intéressées

L'organisation doit déterminer:

a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information; et

b) les exigences de ces parties intéressées concernant la sécurité de l'information.

NOTE Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.

Lorsqu'elle établit ce domaine d'application, l'organisation doit prendre en compte:

a) les enjeux externes et internes auxquels il est fait référence en 4.1;

b) les exigences auxquelles il est fait référence en 4.2; et

c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.

Le domaine d'application doit être disponible sous forme d'information documentée.

4.4 Système de management de la sécurité de l'information

L'organisation doit établir, mettre en œuvre, tenir à jour et améliorer continuellement un système de management de la sécurité de l'information, conformément aux exigences de la présente Norme internationale.

5 Leadership

5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en:

a) s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation;

b) s'assurant que les exigences liées au système de management de la sécurité de l'information sont intégrées aux processus métiers de l'organisation;

c) s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles;

d) communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information;

e) s'assurant que le système de management de la sécurité de l'information produit le ou les résultats escomptés;

f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la sécurité de l'information;

g) promouvant l'amélioration continue; et

h) aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui:

a) est adaptée à la mission de l'organisation;

b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs;

c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information; et

d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.

La politique de sécurité de l'information doit:

e) être disponible sous forme d'information documentée;

f) être communiquée au sein de l'organisation; et

g) être mise à la disposition des parties intéressées, le cas échéant.

5.3 Rôles, responsabilités et autorités au sein de l'organisation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de:

a) s'assurer que le système de management de la sécurité de l'information est conforme aux exigences de la présente Norme internationale; et

b) rendre compte à la direction des performances du système de management de la sécurité de l'information.

NOTE La direction peut également attribuer des responsabilités et autorités pour rendre compte des performances du système de management de la sécurité de l'information au sein de l'organisation.

6 Planification

6.1 Actions liées aux risques et opportunités

6.1.1 Généralités

Lorsqu'elle conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux de 4.1 et des exigences de 4.2, et déterminer les risques et opportunités qui nécessitent d'être abordés pour:

a) s'assurer que le système de management de la sécurité de l'information peut atteindre le ou les résultats escomptés;

b) empêcher ou limiter les effets indésirables; et

c) appliquer une démarche d'amélioration continue.

L'organisation doit planifier:

d) les actions menées pour traiter ces risques et opportunités; et

e) la manière:

   1) d'intégrer et de mettre en œuvre les actions au sein des processus du système de management de la sécurité de l'information; et

   2) d'évaluer l'efficacité de ces actions.

6.1.2 Appréciation des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui:

a) établit et tient à jour les critères de risque de sécurité de l'information incluant:

   1) les critères d'acceptation des risques;

   2) les critères de réalisation des appréciations des risques de sécurité de l'information;

b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables;

c) identifie les risques de sécurité de l'information:

   1) applique le processus d'appréciation des risques de sécurité de l'information pour identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité des informations entrant dans le domaine d'application du système de management de la sécurité de l'information; et

   2) identifie les propriétaires des risques;

d) analyse les risques de sécurité de l'information:

   1) apprécie les conséquences potentielles dans le cas où les risques identifiés en 6.1.2 c) 1) se concrétisaient;

   2) procède à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés en 6.1.2 c) 1); et

   3) détermine les niveaux des risques;

e) évalue les risques de sécurité de l'information:

   1) compare les résultats d'analyse des risques avec les critères de risque déterminés en 6.1.2 a); et

   2) priorise les risques analysés pour le traitement des risques.

L'organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

6.1.3 Traitement des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour:

a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques;

b) déterminer toutes les mesures nécessaires à la mise en œuvre de(s) (l')option(s) de traitement des risques de sécurité de l'information choisie(s);

   NOTE Les organisations peuvent concevoir ces mesures, le cas échéant, ou bien les identifier à partir de n'importe quelle source.

c) comparer les mesures déterminées ci-dessus en 6.1.3 b) avec celles de l'Annexe A et vérifier qu'aucune mesure nécessaire n'a été omise;

   NOTE 1 L'Annexe A comporte une liste détaillée d'objectifs et de mesures. Les utilisateurs de la présente Norme internationale sont invités à se reporter à l'Annexe A pour s'assurer qu'aucune mesure nécessaire n'a été négligée.

   NOTE 2 Les objectifs sont implicitement inclus dans les mesures choisies. Les objectifs et les mesures énumérés dans l'Annexe A ne sont pas exhaustifs et des objectifs et des mesures additionnels peuvent s'avérer nécessaires.

d) produire une déclaration d'applicabilité contenant les mesures nécessaires (voir 6.1.3 b) et c)) et la justification de leur insertion, le fait qu'elles soient mises en œuvre ou non, et la justification de l'exclusion de mesures de l'Annexe A;

e) élaborer un plan de traitement des risques de sécurité de l'information; et

f) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.

L'organisation doit conserver des informations documentées sur le processus de traitement des risques de sécurité de l'information.

NOTE L'appréciation des risques de sécurité de l'information et le processus de traitement figurant dans la présente Norme internationale s'alignent sur les principes et les lignes directrices générales fournies dans l'ISO 31000.[5]

6.2 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information.

Les objectifs de sécurité de l'information doivent:

a) être cohérents avec la politique de sécurité de l'information;

b) être mesurables (si possible);

c) tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques;

d) être communiqués; et

e) être mis à jour quand cela est approprié.

L'organisation doit conserver des informations documentées sur les objectifs liés à la sécurité de l'information.

Lorsqu'elle planifie la façon d'atteindre ses objectifs de sécurité de l'information, l'organisation doit déterminer:

f) ce qui sera fait;

g) les ressources qui seront nécessaires;

h) qui sera responsable;

i) les échéances; et

j) la façon dont les résultats seront évalués.

7 Support

7.1 Ressources

L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.

7.2 Compétence

L'organisation doit:

a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information;

b) s'assurer que ces personnes sont compétentes sur la base d'une formation initiale ou continue ou d'une expérience appropriée;

c) le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises; et

d) conserver des informations documentées appropriées comme preuves de ces compétences.

NOTE Les actions envisageables peuvent notamment inclure la formation, l'encadrement ou la réaffectation du personnel actuellement employé ou le recrutement, direct ou en sous-traitance, de personnes compétentes.

7.3 Sensibilisation

Les personnes effectuant un travail sous le contrôle de l'organisation doivent:

a) être sensibilisées à la politique de sécurité de l'information;

b) avoir conscience de leur contribution à l'efficacité du système de management de la sécurité de l'information, y compris aux effets positifs d'une amélioration des performances de la sécurité de l'information; et

c) avoir conscience des implications de toute non-conformité aux exigences requises par le système de management de la sécurité de l'information.

7.4 Communication

L'organisation doit déterminer les besoins de communication interne et externe pertinents pour le système de management de la sécurité de l'information, et notamment:

a) sur quels sujets communiquer;

b) à quels moments communiquer;

c) avec qui communiquer;

d) qui doit communiquer; et

e) les processus par lesquels la communication doit s'effectuer.

7.5 Informations documentées

7.5.1 Généralités

Le système de management de la sécurité de l'information de l'organisation doit inclure:

a) les informations documentées exigées par la présente Norme internationale; et

b) les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information.

NOTE L'étendue des informations documentées dans le cadre d'un système de management de la sécurité de l'information peut différer selon l'organisation en fonction de:

1) la taille de l'organisation, ses domaines d'activité et ses processus, produits et services;

2) la complexité des processus et de leurs interactions; et

3) la compétence des personnes.

7.5.2 Création et mise à jour

Quand elle crée et met à jour ses informations documentées, l'organisation doit s'assurer que les éléments suivants sont appropriés:

a) identification et description (par exemple titre, date, auteur, numéro de référence);

b) format (par exemple langue, version logicielle, graphiques) et support (par exemple, papier, électronique); et

c) examen et approbation du caractère approprié et pertinent des informations.

7.5.3 Maîtrise des informations documentées

Les informations documentées exigées par le système de management de la sécurité de l'information et par la présente Norme internationale doivent être contrôlées pour s'assurer:

a) qu'elles sont disponibles et conviennent à l'utilisation, où et quand elles sont nécessaires; et

b) qu'elles sont correctement protégées (par exemple, de toute perte de confidentialité, utilisation inappropriée ou perte d'intégrité).

Pour contrôler les informations documentées, l'organisation doit traiter des activités suivantes, quand elles lui sont applicables:

c) distribution, accès, récupération et utilisation;

d) stockage et conservation, y compris préservation de la lisibilité;

e) contrôle des modifications (par exemple, contrôle des versions); et

f) durée de conservation et suppression.

Les informations documentées d'origine externe que l'organisation juge nécessaires à la planification et au fonctionnement du système de management de la sécurité de l'information doivent être identifiées comme il convient et maîtrisées.

NOTE L'accès implique une décision concernant l'autorisation de consulter les informations documentées uniquement, ou l'autorisation et l'autorité de consulter et modifier les informations documentées, etc.

8 Fonctionnement

8.1 Planification et contrôle opérationnels

L'organisation doit planifier, mettre en œuvre et contrôler les processus nécessaires à la satisfaction des exigences liées à la sécurité de l'information et à la réalisation des actions déterminées en 6.1. L'organisation doit également mettre en œuvre des plans pour atteindre les objectifs de sécurité de l'information définis en 6.2.

L'organisation doit conserver des informations documentées dans une mesure suffisante pour avoir l'assurance que les processus ont été suivis comme prévu.

L'organisation doit contrôler les modifications prévues, analyser les conséquences des modifications imprévues et, si nécessaire, mener des actions pour limiter tout effet négatif.

L'organisation doit s'assurer que les processus externalisés sont définis et contrôlés.

8.2 Appréciation des risques de sécurité de l'information

L'organisation doit réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs sont prévus ou ont lieu, en tenant compte des critères établis en 6.1.2 a).

L'organisation doit conserver des informations documentées sur les résultats des processus d'appréciation des risques de sécurité de l'information.

8.3 Traitement des risques de sécurité de l'information

L'organisation doit mettre en œuvre le plan de traitement des risques de sécurité de l'information.

L'organisation doit conserver des informations documentées sur les résultats du traitement des risques de sécurité de l'information.

9 Évaluation des performances

9.1 Surveillance, mesures, analyse et évaluation

L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information.

L'organisation doit déterminer:

a) ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information;

b) les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon le cas, pour assurer la validité des résultats;

NOTE Il convient que les méthodes choisies donnent des résultats comparables et reproductibles pour être considérées comme valables.

c) quand la surveillance et les mesures doivent être effectuées;

d) qui doit effectuer la surveillance et les mesures;

e) quand les résultats de la surveillance et des mesures doivent être analysés et évalués; et

f) qui doit analyser et évaluer ces résultats.

L'organisation doit conserver les informations documentées appropriées comme preuves des résultats de la surveillance et des mesures.

9.2 Audit interne

L'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management de la sécurité de l'information:

a) est conforme:

   1) aux exigences propres de l'organisation concernant son système de management de la sécurité de l'information; et

   2) aux exigences de la présente Norme internationale;

b) est efficacement mis en œuvre et tenu à jour.

L'organisation doit:

c) planifier, établir, mettre en œuvre et tenir à jour un ou plusieurs programmes d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et l'élaboration des rapports. Le ou les programmes d'audit doivent tenir compte de l'importance des processus concernés et des résultats des audits précédents;

d) définir les critères d'audit et le périmètre de chaque audit;

e) sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit;

f) s'assurer qu'il est rendu compte des résultats des audits à la direction concernée; et

g) conserver des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

9.3 Revue de direction

À des intervalles planifiés, la direction doit procéder à la revue du système de management de la sécurité de l'information mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de direction doit prendre en compte:

a) l'état d'avancement des actions décidées à l'issue des revues de direction précédentes;

b) les modifications des enjeux externes et internes pertinents pour le système de management de la sécurité de l'information;

c) les retours sur les performances de sécurité de l'information, y compris les tendances concernant:

   1) les non-conformités et les actions correctives;

   2) les résultats de l'évaluation de la surveillance et des mesures;

   3) les résultats d'audit; et

   4) la réalisation des objectifs en matière de sécurité de l'information;

d) les retours d'information des parties intéressées;

e) les résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques; et

f) les opportunités d'amélioration continue.

Les conclusions de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et aux éventuels changements à apporter au système de management de la sécurité de l'information.

L'organisation doit conserver des informations documentées comme preuves des conclusions des revues de direction.

10 Amélioration

10.1 Non-conformité et actions correctives

Lorsqu'une non-conformité se produit, l'organisation doit:

a) réagir à la non-conformité, et le cas échéant:

   1) agir pour la maîtriser et la corriger; et

2) traiter les conséquences;

b) évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs. À cet effet, l'organisation:

1) examine la non-conformité;

2) détermine les causes de non-conformité; et

3) détermine si des non-conformités similaires existent, ou pourraient se produire;

c) mettre en œuvre toutes les actions requises;

d) réviser l'efficacité de toute action corrective mise en œuvre; et

e) modifier, si nécessaire, le système de management de sécurité de l'information.

Les actions correctives doivent être à la mesure des effets des non-conformités rencontrées.

L'organisation doit conserver des informations documentées comme preuves:

f) de la nature des non-conformités et de toute action subséquente; et

g) des résultats de toute action corrective.

10.2 Amélioration continue

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management de la sécurité de l'information.

Annexe A
(normative)

Objectifs et mesures de référence

Les objectifs et les mesures énumérés dans le Tableau A.1 découlent directement de ceux qui sont répertoriés dans la norme ISO/CEI 27002:2013,[1] Articles 5 à 18, avec lesquels ils sont en adéquation, et doivent être utilisés dans le contexte du paragraphe 6.1.3.

Tableau A.1 — Objectifs et mesures

A.5	**Politiques de sécurité de l'information**	
A.5.1	**Orientations de la direction en matière de sécurité de l'information**	
Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Politiques de sécurité de l'information	*Mesure* Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.
A.5.1.2	Revue des politiques de sécurité de l'information	*Mesure* Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.
A.6	**Organisation de la sécurité de l'information**	
A.6.1	**Organisation interne**	
Objectif: Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation.		
A.6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	*Mesure* Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.
A.6.1.2	Séparation des tâches	*Mesure* Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.
A.6.1.3	Relations avec les autorités	*Mesure* Des relations appropriées avec les autorités compétentes doivent être entretenues.
A.6.1.4	Relations avec des groupes de travail spécialisés	*Mesure* Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues.
A.6.1.5	La sécurité de l'information dans la gestion de projet	*Mesure* La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné.
A.6.2	**Appareils mobiles et télétravail**	
Objectif: Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.		

Tableau A.1 *(suite)*

A.6.2.1	Politique en matière d'appareils mobiles	*Mesure* Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles.
A.6.2.2	Télétravail	*Mesure* Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.
A.7	**Sécurité des ressources humaines**	
A.7.1	**Avant l'embauche**	
Objectif: S'assurer que les salariés et les sous-traitants comprennent leurs responsabilités et sont qualifiés pour les rôles qu'on envisage de leur donner.		
A.7.1.1	Sélection des candidats	*Mesure* Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
A.7.1.2	Termes et conditions d'embauche	*Mesure* Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.
A.7.2	**Pendant la durée du contrat**	
Objectif: S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.		
A.7.2.1	Responsabilités de la direction	*Mesure* La direction doit demander à tous les salariés et sous-traitants d'appliquer les règles de sécurité de l'information conformément aux politiques et aux procédures en vigueur dans l'organisation.
A.7.2.2	Sensibilisation, apprentissage et formation à la sécurité de l'information	*Mesure* L'ensemble des salariés de l'organisation et, quand cela est pertinent, des sous-traitants, doit bénéficier d'une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.
A.7.2.3	Processus disciplinaire	*Mesure* Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.
A.7.3	**Rupture, terme ou modification du contrat de travail**	
Objectif: Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.		
A.7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail	*Mesure* Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, doivent être définies, communiquées au salarié ou au sous-traitant, et appliquées.
A.8	**Gestion des actifs**	
A.8.1	**Responsabilités relatives aux actifs**	
Objectif: Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée.		

Tableau A.1 *(suite)*

A.8.1.1	Inventaire des actifs	*Mesure* Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.
A.8.1.2	Propriété des actifs	*Mesure* Les actifs figurant à l'inventaire doivent être attribués à un propriétaire.
A.8.1.3	Utilisation correcte des actifs	*Mesure* Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre.
A.8.1.4	Restitution des actifs	*Mesure* Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.
A.8.2 Classification de l'information		
Objectif: S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.		
A.8.2.1	Classification des informations	*Mesure* Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.
A.8.2.2	Marquage des informations	*Mesure* Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation.
A.8.2.3	Manipulation des actifs	*Mesure* Des procédures de traitement de l'information doivent être élaborées et mises en œuvre conformément au plan de classification de l'information adopté par l'organisation.
A.8.3 Manipulation des supports		
Objectif: Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.		
A.8.3.1	Gestion des supports amovibles	*Mesure* Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l'organisation.
A.8.3.2	Mise au rebut des supports	*Mesure* Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles.
A.8.3.3	Transfert physique des supports	*Mesure* Les supports contenant de l'information doivent être protégés contre les accès non autorisés, les erreurs d'utilisation et l'altération lors du transport.
A.9 Contrôle d'accès		
A.9.1 Exigences métier en matière de contrôle d'accès		
Objectif: Limiter l'accès à l'information et aux moyens de traitement de l'information.		
A.9.1.1	Politique de contrôle d'accès	*Mesure* Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.

Tableau A.1 *(suite)*

A.9.1.2	Accès aux réseaux et aux services réseau	*Mesure* Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation.
A.9.2 Gestion de l'accès utilisateur		
Objectif: Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.		
A.9.2.1	Enregistrement et désinscription des utilisateurs	*Mesure* Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.
A.9.2.2	Distribution des accès aux utilisateurs	*Mesure* Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes.
A.9.2.3	Gestion des droits d'accès à privilèges	*Mesure* L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.
A.9.2.4	Gestion des informations secrètes d'authentification des utilisateurs	*Mesure* L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.
A.9.2.5	Revue des droits d'accès utilisateurs	*Mesure* Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.
A.9.2.6	Suppression ou adaptation des droits d'accès	*Mesure* Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.
A.9.3 Responsabilités des utilisateurs		
Objectif: Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.		
A.9.3.1	Utilisation d'informations secrètes d'authentification	*Mesure* Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.
A.9.4 Contrôle de l'accès au système et à l'information		
Objectif: Empêcher les accès non autorisés aux systèmes et aux applications.		
A.9.4.1	Restriction d'accès à l'information	*Mesure* L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.
A.9.4.2	Sécuriser les procédures de connexion	*Mesure* Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.
A.9.4.3	Système de gestion des mots de passe	*Mesure* Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe.
A.9.4.4	Utilisation de programmes utilitaires à privilèges	*Mesure* L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.

Tableau A.1 *(suite)*

A.9.4.5	Contrôle d'accès au code source des programmes	*Mesure* L'accès au code source des programmes doit être restreint.
A.10 Cryptographie		
A.10.1 Mesures cryptographiques		
Objectif: Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.		
A.10.1.1	Politique d'utilisation des mesures cryptographiques	*Mesure* Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.
A.10.1.2	Gestion des clés	*Mesure* Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie.
A.11 Sécurité physique et environnementale		
A.11.1 Zones sécurisées		
Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.		
A.11.1.1	Périmètre de sécurité physique	*Mesure* Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.
A.11.1.2	Contrôle d'accès physique	*Mesure* Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.
A.11.1.3	Sécurisation des bureaux, des salles et des équipements	*Mesure* Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.
A.11.1.4	Protection contre les menaces extérieures et environnementales	*Mesure* Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.
A.11.1.5	Travail dans les zones sécurisées	*Mesure* Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées.
A.11.1.6	Zones de livraison et de chargement	*Mesure* Les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.
A.11.2 Matériels		
Objectif: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.		
A.11.2.1	Emplacement et protection des matériels	*Mesure* Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.

Tableau A.1 *(suite)*

A.11.2.2	Services généraux	*Mesure* Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux.
A.11.2.3	Sécurité du câblage	*Mesure* Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage.
A.11.2.4	Maintenance des matériels	*Mesure* Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité.
A.11.2.5	Sortie des actifs	*Mesure* Les matériels, les informations ou les logiciels des locaux de l'organisation ne doivent pas sortir sans autorisation préalable.
A.11.2.6	Sécurité des matériels et des actifs hors des locaux	*Mesure* Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.
A.11.2.7	Mise au rebut ou recyclage sécurisé(e) des matériels	*Mesure* Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.
A.11.2.8	Matériels utilisateur laissés sans surveillance	*Mesure* Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.
A.11.2.9	Politique du bureau propre et de l'écran verrouillé	*Mesure* Une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran verrouillé pour les moyens de traitement de l'information doivent être adoptées.
A.12	**Sécurité liée à l'exploitation**	
A.12.1	**Procédures et responsabilités liées à l'exploitation**	
Objectif: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.		
A.12.1.1	Procédures d'exploitation documentées	*Mesure* Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.
A.12.1.2	Gestion des changements	*Mesure* Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.
A.12.1.3	Dimensionnement	*Mesure* L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.
A.12.1.4	Séparation des environnements de développement, de test et d'exploitation	*Mesure* Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.
A.12.2	**Protection contre les logiciels malveillants**	

Tableau A.1 *(suite)*

Objectif: S'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants.		
A.12.2.1	Mesures contre les logiciels malveillants	*Mesure* Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.
A.12.3 Sauvegarde		
Objectif: Se protéger de la perte de données.		
A.12.3.1	Sauvegarde des informations	*Mesure* Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.
A.12.4 Journalisation et surveillance		
Objectif: Enregistrer les événements et générer des preuves.		
A.12.4.1	Journalisation des événements	*Mesure* Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.
A.12.4.2	Protection de l'information journalisée	*Mesure* Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé.
A.12.4.3	Journaux administrateur et opérateur	*Mesure* Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.
A.12.4.4	Synchronisation des horloges	*Mesure* Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.
A.12.5 Maîtrise des logiciels en exploitation		
Objectif: Garantir l'intégrité des systèmes en exploitation.		
A.12.5.1	Installation de logiciels sur des systèmes en exploitation	*Mesure* Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur des systèmes en exploitation.
A.12.6 Gestion des vulnérabilités techniques		
Objectif: Empêcher toute exploitation des vulnérabilités techniques.		
A.12.6.1	Gestion des vulnérabilités techniques	*Mesure* Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.
A.12.6.2	Restrictions liées à l'installation de logiciels	*Mesure* Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.
A.12.7 Considérations sur l'audit des systèmes d'information		
Objectif: Réduire au minimum l'impact des activités d'audit sur les systèmes en exploitation.		

Tableau A.1 *(suite)*

A.12.7.1	Mesures relatives à l’audit des systèmes d’information	*Mesure* Les exigences et activités d’audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.
A.13 Sécurité des communications		
A.13.1 Gestion de la sécurité des réseaux		
Objectif: Garantir la protection de l’information sur les réseaux et des moyens de traitement de l’information sur lesquels elle s’appuie.		
A.13.1.1	Contrôle des réseaux	*Mesure* Les réseaux doivent être gérés et contrôlés pour protéger l’information contenue dans les systèmes et les applications.
A.13.1.2	Sécurité des services de réseau	*Mesure* Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
A.13.1.3	Cloisonnement des réseaux	*Mesure* Les groupes de services d’information, d’utilisateurs et de systèmes d’information doivent être cloisonnés sur les réseaux.
A.13.2 Transfert de l’information		
Objectif: Maintenir la sécurité de l’information transférée au sein de l’organisme et vers une entité extérieure.		
A.13.2.1	Politiques et procédures de transfert de l’information	*Mesure* Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d’information transitant par tous types d’équipements de communication.
A.13.2.2	Accords en matière de transfert d’information	*Mesure* Des accords doivent traiter du transfert sécurisé de l’information liée à l’activité entre l’organisation et les tiers.
A.13.2.3	Messagerie électronique	*Mesure* L’information transitant par la messagerie électronique doit être protégée de manière appropriée.
A.13.2.4	Engagements de confidentialité ou de non-divulgation	*Mesure* Les exigences en matière d’engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l’organisation.
A.14 Acquisition, développement et maintenance des systèmes d’information		
A.14.1 Exigences de sécurité applicables aux systèmes d’information		
Objectif: Veiller à ce que la sécurité de l’information fasse partie intégrante des systèmes d’information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d’information fournissant des services sur les réseaux publics.		
A.14.1.1	Analyse et spécification des exigences de sécurité de l’information	*Mesure* Les exigences liées à la sécurité de l’information doivent être intégrées aux exigences des nouveaux systèmes d’information ou des améliorations de systèmes d’information existants.

Tableau A.1 *(suite)*

A.14.1.2	Sécurisation des services d'application sur les réseaux publics	*Mesure* Les informations liées aux services d'application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents contractuels, ainsi que la divulgation et la modification non autorisées.
A.14.1.3	Protection des transactions liées aux services d'application	*Mesure* Les informations impliquées dans les transactions liées aux services d'application doivent être protégées pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.
A.14.2 Sécurité des processus de développement et d'assistance technique		
Objectif: S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.		
A.14.2.1	Politique de développement sécurisé	*Mesure* Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation.
A.14.2.2	Procédures de contrôle des changements de système	*Mesure* Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.
A.14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation	*Mesure* Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
A.14.2.4	Restrictions relatives aux changements apportés aux progiciels	*Mesure* Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé.
A.14.2.5	Principes d'ingénierie de la sécurité des systèmes	*Mesure* Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.
A.14.2.6	Environnement de développement sécurisé	*Mesure* Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.
A.14.2.7	Développement externalisé	*Mesure* L'organisation doit superviser et contrôler l'activité de développement du système externalisée.
A.14.2.8	Test de la sécurité du système	*Mesure* Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.
A.14.2.9	Test de conformité du système	*Mesure* Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.
A.14.3 Données de test		
Objectif: Garantir la protection des données utilisées pour les tests.		

Tableau A.1 *(suite)*

A.14.3.1	Protection des données de test	*Mesure* Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.
A.15 Relations avec les fournisseurs		
A.15.1 Sécurité dans les relations avec les fournisseurs		
Objectif: Garantir la protection des actifs de l'organisation accessible aux fournisseurs.		
A.15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	*Mesure* Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être acceptées par le fournisseur et documentées.
A.15.1.2	La sécurité dans les accords conclus avec les fournisseurs	*Mesure* Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.
A.15.1.3	Chaîne d'approvisionnement des produits et des services informatiques	*Mesure* Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques.
A.15.2 Gestion de la prestation du service		
Objectif: Maintenir le niveau convenu de sécurité de l'information et de service conforme aux accords conclus avec les fournisseurs.		
A.15.2.1	Surveillance et revue des services des fournisseurs	*Mesure* Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.
A.15.2.2	Gestion des changements apportés dans les services des fournisseurs	*Mesure* Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.
A.16 Gestion des incidents liés à la sécurité de l'information		
A.16.1 Gestion des incidents liés à la sécurité de l'information et améliorations		
Objectif: Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.		
A.16.1.1	Responsabilités et procédures	*Mesure* Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.
A.16.1.2	Signalement des événements liés à la sécurité de l'information	*Mesure* Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.
A.16.1.3	Signalement des failles liées à la sécurité de l'information	*Mesure* Les salariés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Tableau A.1 *(suite)*

A.16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision	*Mesure* Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information.
A.16.1.5	Réponse aux incidents liés à la sécurité de l'information	*Mesure* Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.
A.16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information	*Mesure* Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.
A.16.1.7	Collecte de preuves	*Mesure* L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.
A.17	**Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité**	
A.17.1	**Continuité de la sécurité de l'information**	
Objectif: La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité.		
A.17.1.1	Organisation de la continuité de la sécurité de l'information	*Mesure* L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre
A.17.1.2	Mise en œuvre de la continuité de la sécurité de l'information	*Mesure* L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.
A.17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information	*Mesure* L'organisation doit vérifier les mesures de continuité de la sécurité de l'information mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables.
A.17.2	**Redondances**	
Objectif: Garantir la disponibilité des moyens de traitement de l'information		
A.17.2.1	Disponibilité des moyens de traitement de l'information	*Mesure* Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.
A.18	**Conformité**	
A.18.1	**Conformité aux obligations légales et réglementaires**	
Objectif: Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.		
A.18.1.1	Identification de la législation et des exigences contractuelles applicables	*Mesure* Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisation elle-même.

Tableau A.1 *(suite)*

A.18.1.2	Droits de propriété intellectuelle	*Mesure* Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.
A.18.1.3	Protection des enregistrements	*Mesure* Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.
A.18.1.4	Protection de la vie privée et protection des données à caractère personnel	*Mesure* La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.
A.18.1.5	Réglementation relative aux mesures cryptographiques	*Mesure* Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables.
A.18.2 Revue de la sécurité de l'information		
Objectif: Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.		
A.18.2.1	Revue indépendante de la sécurité de l'information	*Mesure* Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.
A.18.2.2	Conformité avec les politiques et les normes de sécurité	*Mesure* Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.
A.18.2.3	Vérification de la conformité technique	*Mesure* Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.

Bibliographie

[1] ISO/CEI 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

[2] ISO/CEI 27003, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information*

[3] ISO/CEI 27004, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Mesurage*

[4] ISO/CEI 27005, *Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information*

[5] ISO 31000:2009, *Management du risque — Principes et lignes directrices*

[6] Directives ISO/CEI, Partie 1, *Supplément ISO consolidé — Procédures spécifiques à l'ISO*, 2012